Tanya Gärtner, Annika Selzer

Metrikensysteme als Beitrag zur Umsetzung des risikobasierten Ansatzes

Angemessene Umsetzung des technisch- organisatorischen Datenschutzes durch Metrikensysteme

Der risikobasierte Ansatz ist ein prägendes Merkmal der DSGVO. Eine einwandfreie und präzise Umsetzung dieses Grundsatzes lässt Effizienzgewinne für Verantwortliche erwarten, ohne gleichzeitig ein adäquates Schutzniveau für betroffene Personen zu gefährden. Der vorliegende Beitrag untersucht, ob in dieser Hinsicht Optimierungspotential in Bezug auf Datenschutzaudits besteht und inwiefern hierfür neue Technologien nützlich gemacht werden können. Dafür wird der Prozess des Datenschutzaudits analysiert und auf eine Einsatzfähigkeit von Datenschutzmetriken hin untersucht.

1 Fragestellung[1]

Das zentrale Element des risikobasierten Ansatzes der DSGVO ist es, die Höhe des Risikos für die Rechte und Freiheiten der betroffenen Personen unmittelbar mit Art und Umfang der zum Schutz der betroffenen Personen getroffenen technischen und organisatorischen Maßnahmen zu verknüpfen. Auf Basis einer Einschätzung der Risikointensität für die Rechte und Freiheiten der betroffenen Personen sollen technische und organisatorische Maßnahmen getroffen werden, die die betroffenen Personen vor den mit der Datenverarbeitung einhergehenden Risiken *angemessen* schützen. Somit erfordert eine besonders risikobehaftete Datenverarbeitung regelmäßig ein höheres Maß technischer und organisatorischer Maßnahmen als eine Datenverarbeitung mit mäßigen Risiken.[2]

Datenschutzmetriken sind ein Monitoring-Instrument, mit dessen Hilfe sich der Umsetzungsgrad datenschutzrechtlicher Anforderungen systematisch und automatisiert (bzw. teilautomatisiert) bewerten lässt. Einen Schwerpunkt des Monitorings durch Datenschutzmetriken bildet die Umsetzung technischer und organisatorischer Maßnahmen.

Vor diesem Hintergrund untersucht der vorliegende Beitrag, inwiefern die Umsetzung des risikobasierten Ansatzes durch Datenschutzmetriken unterstützt und optimiert werden kann. Hierfür wird zunächst der risikobasierte Ansatz der DSGVO näher dargestellt (2), bevor Datenschutzaudits und dessen Ergebnisse als Basis fortlaufender Anpassung von Datenschutzmaßnahmen im Sinne des risikobasierten Ansatzes skizziert (3) sowie Alternativen zu „klassischen" Audits vorgestellt (4), diskutiert (5) und als Unterstützung der Umsetzung des risikobasierten Ansatzes motiviert (6) werden.

1 Die diesem Beitrag zugrundeliegenden Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projektes Edumida, 16KIS1361K, und vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autorinnen wieder.

Tanya Gärtner

ist Wissenschaftlerin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) und am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE. Ihre Forschungsschwerpunkte liegen im Datenschutzrecht sowie im Recht der IT-Sicherheitsforschung, insbesondere zu völkerrechtlichen Fragen.
E-Mail: tanya.gaertner@sit.fraunhofer.de

Dr. Annika Selzer

ist Abteilungsleiterin am Fraunhofer SIT und Co-Forschungsbereichskoordinatorin sowie Principal Investigator in ATHENE.

E-Mail: annika.selzer@sit.fraunhofer.de

2 *Schröder*, ZD 2019, 503 (503 f.); *Heberlein* in *Ehmann/Selmayr*, DSGVO-Kommentar, Art. 5 Rdnr. 30; *Gola/Klug*, NJW 2018, 2608 (2609). *Selzer/Woods/Böhme*, EDPL 2021, 456 (456 f.); *Selzer/ Timm*, Angemessene technische und organisatorische Schutzmaßnahmen nach Art. 32 DSGVO – Ein Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen, HMD Praxis der Wirtschaftsinformatik (online first).

2 Risikobasierter Ansatz der DSGVO

Die Berücksichtigung des Risikos für die Rechte und Freiheiten betroffener Personen im Rahmen der Umsetzung datenschutzrechtlicher Vorgaben ist nicht gänzlich neu: Vor Geltung der DSGVO regelte die DSRL u.a. das Instrument der Vorabkontrolle sowie die Angemessenheit technischer und organisatorischer Maßnahmen als erste „Anzeichen" des risikobasierten Ansatzes der DSGVO.[3] Mit Geltungsbeginn der DSGVO im Mai 2018 wurde der risikobasierte Ansatz sodann erstmals explizit Teil des Europäischen Datenschutzrechts.

2.1 Normative Verankerung

Der für die Datenverarbeitung Verantwortliche[4] unterliegt gemäß Art. 24 Abs. 1 S. 1 DSGVO der Verpflichtung, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. Folglich muss ein Verantwortlicher zuerst die in Art. 24 Abs. 1 S. 1 DSGVO genannten Kriterien heranziehen, um das aufgrund der Datenverarbeitung bestehende Risiko für die Rechte und Freiheiten der betroffenen Personen zu bewerten.[5] Abhängig vom Ergebnis können dann technische und organisatorische Maßnahmen bestimmt werden, um das Risiko abzuwenden.[6] Der risikobasierte Ansatz der DSGVO ermöglicht also eine Skalierung der zu ergreifenden Maßnahmen in Abhängigkeit von dem bestehenden Risiko.[7] Je höher der Schutzbedarf der Rechte und Freiheiten der betroffenen Personen ist, desto höher ist demnach der zumutbare Aufwand für den Verantwortlichen.[8]

2.2 Risikobegriff

Vor dem Hintergrund der zentralen Rolle, die das Risiko für die Rechte und Freiheiten natürlicher Personen einnimmt, stellt sich die Frage, was genau hierunter zu verstehen ist. Die DSGVO hält für den Begriff des Risikos keine Definition bereit. Auch die Erwgr. 75 und 76 DSGVO schaffen diesbezüglich wenig Abhilfe und stellen lediglich klar, dass ein Risiko aus einer Verarbeitung personenbezogener Daten hervorgehen kann, die zu einem physischen, materiellen oder immateriellen Schaden führen kann, und dass das Risiko anhand einer objektiven Bewertung beurteilt werden sollte. In Anbetracht dieser Ungenauigkeit wird die Ansicht vertreten, dass der risikobasierte Ansatz folglich für Verantwortliche, die sicher gehen wollen, den Anforderungen der DGSVO zu genügen, eher zu einer Ausweitung ihrer Pflichten führen könnte, anstatt zu einer sinnvollen Abstufung dergleichen.[9]

2.3 Kernelemente

Der risikobasierte Ansatz wird an weiteren Stellen der DSGVO aufgegriffen und weiterentwickelt.[10] So stellt z. B. Art. 25 Abs. 1 DSGVO[11] klar, dass technische und organisatorische Maßnahmen bereits in angemessener Weise in die Technikgestaltung einfließen müssen und hierbei insbesondere die für die betroffenen Personen bestehenden Risiken zu berücksichtigen sind („Data Protection by Design")". Die Auswahl geeigneter technischer und organisatorischer Maßnahmen wird in Art. 32 DSGVO dahingehend konkretisiert[12], dass auch der Stand der Technik und die Implementierungskosten beachtet werden müssen. Der risikobasierte Ansatz schlägt sich auch in der Pflicht des Datenschutzbeauftragten in Art. 39 Abs. 2 DSGVO nieder[13], bei der Erfüllung seiner Aufgaben dem mit den Datenverarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen.

Als Kernelement[14] des risikobasierten Ansatzes sieht Art. 35 DSGVO eine Datenschutz-Folgenabschätzung vor, die der Verantwortliche durchzuführen hat, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Für den Fall, dass eine Verletzung des Schutzes personenbezogener Daten vorgefallen ist und dies voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen mit sich bringt, muss der Verantwortliche die betroffene Person gemäß Art. 34 Abs. 1 DSGVO hierüber benachrichtigen. Bereits bei einem (normalen) Risiko für die natürliche Person besteht für den Verantwortlichen eine Pflicht zur Meldung der Verletzung gegenüber der zuständigen Aufsichtsbehörde, Art. 33 Abs. 1 DSGVO.

Schlussendlich ist es für die fortlaufende Anpassung von Datenschutzmaßnahmen im Sinne des risikobasierten Ansatzes erforderlich, sich regelmäßig über den Umsetzungsstand der umgesetzten technischen und organisatorischen Maßnahmen zu informieren. Dies erfolgt i.d.R. im Rahmen von Datenschutzaudits.

3 „Klassische" Datenschutzaudits

„Klassische" Datenschutzaudits werden durchgeführt, um die datenschutzkonforme Umsetzung der für eine Organisation einschlägigen Datenschutzgesetze in regelmäßigen Abständen (z.B. jährlich oder zweijährlich) zu überprüfen. Auch für evtl. im Laufe der Zeit notwendig werdende Anpassungen der initial implementieren Datenschutzmaßnahmen im Sinne des risikobasierten Ansatzes ist ein konkreter und aktueller Wissensstand über die Wirksamkeit und Angemessenheit der Maßnahmen erforderlich. Datenschutzaudits lassen sich hinsichtlich der das Audit durchführenden Stelle unterscheiden.

3.1 Interne Audits

Bei internen Audits wird das gesamte Audit umgesetzt, ohne organisationsexterne Personen in diesen Vorgang einzubinden. Das Audit wird ausschließlich von Mitarbeitern der eigenen Organisation durchgeführt, die verschiedene Aspekte der Datenschutz-

3 *Heberlein* in *Ehmann/Selmayr*, DSGVO-Kommentar, Art. 5 Rdnr. 30.
4 Im vorliegenden Beitrag werden die Begriffe „Verantwortlicher" und (zu überprüfende) „Organisation" als Synonyme verwendet.
5 *Piltz* in *Gola*, DSGVO, Art. 24 Rdnr. 19-20.
6 *Lang* in *Taeger/Gabel*, DSGVO/BDSG/TTDSG, Art. 24 Rdnr. 33.
7 *Lang* in *Taeger/Gabel*, DSGVO/BDSG/TTDSG, Art. 24 Rdnr. 32.
8 *Veil*, ZD 2018, 9 (13).
9 *Schröder*, ZD 2019, 503 (505).
10 *Hartung* in *Kühling/Buchner*, DSGVO/BDSG, Art. 24 Rdnr. 1, m. w. N.
11 *Lang* in *Taeger/Gabel*, DSGVO/BDSG/TTDSG, Art. 24 Rdnr. 15.
12 *Lang* in *Taeger/Gabel*, DSGVO/BDSG/TTDSG, Art. 24 Rdnr. 15.
13 *Paal* in *Paal/Pauly*, DSGVO/BDSG, Art. 39 Rdnr. 10.
14 *Martini* in *Paal/Pauly*, DSGVO/BDSG, Art. 24 Rdnr. 2.

umsetzung händisch überprüfen. Beispielsweise kann im Rahmen eines solchen Audits überprüft werden,

- ob die Organisation personenbezogene Daten nur auf Basis einschlägiger Rechtsgrundlagen verarbeitet und diese ausreichend dokumentiert sind,
- ob die Organisation die betroffenen Personen ausreichend über bevorstehende Datenverarbeitungen informiert,
- ob ggf. notwendige Verträge über Auftragsverarbeitungen oder gemeinsame datenschutzrechtliche Verantwortlichkeiten geschlossen wurden,
- ob die Zwecke der Datenverarbeitung ausreichend dokumentiert wurden,
- ob Prozesse zur Umsetzung datenschutzrechtlicher Löschpflichten sowie zur Umsetzung von Betroffenenrechten umgesetzt wurden,
- ob die Mitarbeiter der Organisation regelmäßig und nachweisbar geschult werden und
- ob die Organisation angemessene technische und organisatorische Maßnahmen umsetzt.

Interne Audits werden i.d.R. entweder durch den Datenschutzbeauftragten, ggf. mit Unterstützung des IT-Sicherheitsbeauftragten, oder durch die Innenrevisionsabteilung durchgeführt.

3.2 Externe Audits

Im Unterschied zu internen Audits erfolgt ein externes Audit durch einen von der zu überprüfenden Organisation extern beauftragten Auditor. Die möglichen Prüfbereiche entsprechen denen eines internen Audits.

Der Prüfumfang eines internen oder externen Audits wird vor der Auditdurchführung festgelegt. Je nachdem, welches Ziel mit dem Audit verfolgt wird, ist es möglich, dass ein Audit die (angemessene) Umsetzung der einschlägigen Datenschutzbestimmungen für die gesamte Organisation überprüft oder aber lediglich die (angemessene) Umsetzung einzelner Datenverarbeitungsbereiche (z.B. Personalverwaltung) oder etwaiger Produkte einer Organisation (z.B. Kundenpflegesystem) bewertet.

Sowohl interne als auch externe Audits müssen in der Organisation i.d.R. umfangreich vorbereitet werden. So werden in Vorbereitung des bevorstehenden Audits z.B. häufig Datenschutzdokumentationen, Zugriffsberechtigungskonzepte und Löschregelkataloge auf Aktualität und Vollständigkeit überprüft, die an dem Audit mitwirkenden Mitarbeiter auf die Überprüfung vorbereitet und die umgesetzten technischen und organisatorischen Maßnahmen auf Angemessenheit und Aktualität überprüft.

4 Metrikensystem als Alternative klassischer Audits

Eine zukunftsträchtige Alternative zu den gerade genannten, rein händisch durchgeführten internen oder externen Audits stellen Metrikensysteme für den Datenschutz dar, die eine kontinuierliche Überprüfung des (angemessenen) Datenschutzumsetzungsgrades ermöglichen.[15]

4.1 Metriken und Metrikensysteme

Mittels Metrikensystemen für den Datenschutz kann der (angemessene) Umsetzungsgrad datenschutzrechtlicher Anforderungen systematisch bewertet und aufgezeigt werden. Dies erfolgt mittels automatisierter bzw. teilautomatisierter Datenschutzmetriken.

Bei Datenschutzmetriken handelt es sich um Kennzahlen zur Bewertung datenschutzrelevanter Eigenschaften, die auf einer Auswertung vertrauenswürdiger Messdaten beruhen.[16] Datenschutzmetriken sind also ein Monitoring-Instrument, mit dessen Hilfe

- der aktuelle Zustand eines zu messenden Datenschutzmerkmals analysiert,
- die durch die einschlägigen Datenschutzgesetze vorgegebenen Zielerfüllung gemessen und bewertet und
- Verbesserungspotential identifiziert werden kann.[17]

Ein Metrikensystem für den Datenschutz umfasst die Bewertungen der einzelnen Datenschutzmetriken (z.B. zur Bewertung des Umsetzungsgrades der Datenminimierung, einer einschlägigen Rechtsgrundlage oder der Speicherbegrenzung) und zeigt die Messergebnisse aller Metrikenberechnungen auf. Teil des Metrikensystems ist, als Grundlage der Bewertung der einzelnen Metriken, i.d.R. auch die vertrauenswürdigen Messdatenbasis.

4.2 Anwendungsgebiete und Adressaten

Die Anwendungsgebiete von Metriken sind vielfältig. Bereits aktiv eingesetzt werden Metriken u.a. für die Bewertung von Datensicherheitsanforderungen und ESG-Kriterien (Environment, Social, Governance Anlagekriterien). Im Bereich des Datenschutzrechts wurden Metriken u.a. bereits für den datenschutzkonformen Einsatz von Cloud-Computing-Diensten und für den datenschutzkonformen Mitarbeiterdatenschutz vorgeschlagen und diskutiert.[18]

Metriken können unterschiedliche Zielgruppen haben, u. a. das Management, den Datenschutzbeauftragten und den IT-Sicherheitsbeauftragten,[19] aber auch die Innenrevisionsabteilung einer Organisation. Da im Rahmen eines Metrikensystems die Messergebnisse i.d.R. umfangreich dokumentiert werden, könnten Metrikensysteme u.a. auch zum Nachweis der datenschutzkonformen Umsetzung gegenüber der für eine Organisation zuständigen Datenschutzaufsichtsbehörde genutzt werden. Im Rahmen von Datenschutzmetriken, die den Umsetzungsgrad des Mitarbeiterdatenschutzes verifizieren, können grundsätzlich auch die Mitarbeiter oder der Betriebsrat der Organisation eine Zielgruppe von Datenschutzmetriken sein.

Ähnlich wie händische Audits können Metrikensysteme grundsätzlich so gestaltet werden, dass diese ausschließlich organisationsintern eingesetzt oder durch einen externen Auditor angeboten werden.

15 Selzer, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit, S. 41; Jäger/Selzer/Waldmann, DuD 2015, 26.

16 Jäger/Kraft/Selzer/Waldmann, Werkzeuge zur Messung der datenschutzkonformen Einhaltung des Verarbeitungsstandorts in der Cloud, INFORMATIK 2015 Lecture Notes in Informatics (LNI), S. 525 f.; Jäger/Selzer/Waldmann, DuD 2015, 26.

17 Sowa, Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring, S. 2 ff.; Diel/Kohn/Schleper/Selzer, DuD 2021, 822.

18 U.a. Jäger/Selzer/Waldmann, DuD 2015, 26; Jäger/Kraft/Selzer/Waldmann, DuD 2016, 239; Jäger/Kraft/Selzer/Waldmann, DuD 2016, 305; Diel/Kohn/Schleper/Selzer, DuD 2021, 822.

19 Jäger/Selzer/Waldmann, DuD 2015, 26.

5 Vor- und Nachteile von Metrikensystemen

Metrikensysteme zur Überwachung des Umsetzungsgrades des Datenschutzes könnten händische Datenschutzaudits zukünftig ersetzen. Im direkten Vergleich zu händischen Audits geht dies mit einigen Vor- und Nachteilen einher.

5.1 Nachteile

Da sich aktuell noch nicht sämtliche Datenschutzanforderungen vollständig automatisiert überprüfen lassen, müsste – bis dies vollständig möglich ist – ein interner oder externer Auditor diejenigen Überprüfungen händisch durchführen, die aktuell noch nicht vollständig automatisiert umsetzbar sind.
Darüber hinaus schafft die Ankündigung eines händischen Audits in der Organisation i.d.R. einen hohen Grad an Aufmerksamkeit, der für die von dem Audit betroffenen Abteilungen sogar einen Trainingscharakter haben kann.[20] Es ist davon auszugehen, dass dieser Effekt bei kontinuierlichen Echtzeitaudits im Rahmen eines Metrikensystems nicht bzw. allenfalls stark abgeschwächt eintritt.
Ein weiterer Nachteil eines Metrikensystems ist der Umstand, dass im Vergleich zu händischen Audits deutlich mehr Daten erhoben werden müssen, um die kontinuierliche Auswertung zu ermöglichen. Zwar ist es i.d.R. möglich, die Verarbeitung personenbezogener Daten (z.B. Informationen zu Personen, die sich in einem System eingeloggt haben, Informationen über Administratorentätigkeiten) hierbei vollständig zu unterbinden oder auf ein sehr geringes Maß zu reduzieren und die personenbezogenen Daten durch weitere Maßnahmen wie z.B. Pseudonymisierung oder Verschlüsselung zu schützen, jedoch fallen sie durch das Metrikensystem zusätzlich an oder werden an einem zusätzlichen „Ort" (dem Metrikensystem) gespeichert. Darüber hinaus können kontinuierliche Auswertungen der Systeme dazu führen, dass die ausgewerteten, nicht personenbezogenen Daten Informationen enthalten, die eine Organisation für besonders schützenswert hält, z.B. Serverauslastungen oder Kundenzahlen. Sofern ein Metrikensystem ausschließlich organisationsintern eingesetzt wird, dürften sich hieraus keine Nachteile ergeben. Sollte das Metrikensystem aber durch einen externen Auditor betrieben werden, möchte die Organisation ggf. den Zugriff zu solchen Informationen durch einen externen Auditor unterbinden.

5.2 Vorteile

Bei einem „klassischen" Audit wird lediglich der Ist-Zustand der Datenschutzumsetzung überprüft. Insbesondere für die Überprüfung der Umsetzung technischer und organisatorischer Maßnahmen kann es jedoch von großem Nutzen sein, nicht nur eine Momentaufnahme des Umsetzungsgrades zu erhalten, sondern den Umsetzungsgrad kontinuierlich zu überprüfen. Dies birgt den großen Vorteil, dass Fehler und Lücken in der Umsetzung schnell erkannt werden und unmittelbar auf diese reagiert werden kann. Durch diesen Umstand kann also z.B. eine potenziell große Datenpanne verhindert oder zumindest stark eingedämmt werden, da eine unmittelbare Reaktion auf das in Echtzeit berechnete Metrikenergebnis möglich ist.[21]
Darüber hinaus bergen Metrikensysteme – sobald sie initial implementiert wurden – einen finanziellen Vorteil für die datenschutzrechtlich zu überprüfende Organisation, da automatisierte Audits im Vergleich zu händischen Audits zu einem vergleichsweise kostengünstigen Preis durchgeführt werden können und somit insbesondere auch für kleine und mittelständische Unternehmen einen Mehrwert bieten können, insbesondere dann, wenn sie nicht auf organisationsinternes Audit-Know-How zurückgreifen können.[22]

Des Weiteren lassen sich durch die automatisierte, umfangreiche Dokumentation des Umsetzungsgrades datenschutzrechtlicher Anforderungen im Metrikensystems Anteile der datenschutzrechtlichen Nachweispflichten ohne zusätzlichen Aufwand umsetzen, was zu einer weiteren Entlastung der Organisation führt.

Die Dokumentationen des Metrikensystems können darüber hinaus zielgruppenspezifisch gestaltet werden, so dass die Prüfergebnisse einer großen Anzahl möglicher Zielgruppen bereitgestellt werden können (z.B. betroffenen Personen wie Mitarbeitern, Betriebsräten oder Datenschutzaufsichtsbehörden). Betroffenen Personen, wie z.B. Mitarbeitern, die Möglichkeit zu geben, sich laufend über die datenschutzkonforme Behandlung ihrer personenbezogenen Daten zu informieren, könnte wiederum für einen höheren Grad an Zufriedenheit der betroffenen Personen sorgen – im Bereich des Mitarbeiterdatenschutzes insbesondere in Branchen, in denen die Mitarbeiter häufig zum „gläsernen Mitarbeiter" werden (z.B. durch eine fortlaufende Standortbestimmung in der Logistik).

6 Metrikensysteme als Umsetzungsbeitrag des risikobasierten Ansatzes

Angesichts dessen, dass die Kernfunktion von Metrikensystemen in der Überwachung des Umsetzungsgerades von Datenschutzmaßnahmen liegt, könnte eine kontinuierliche Auditierung auf ihrer Grundlage der Umsetzung des risikobasierten Ansatzes der DSGVO wesentlich Vorschub leisten.

6.1 Allgemeiner Effizienzgewinn

Wie oben dargestellt, ermöglicht der risikobasierte Ansatz der DSGVO eine Skalierung der zu ergreifenden Datenschutzmaßnahmen in Abhängigkeit von der Eintrittswahrscheinlichkeit und Schwere des aufgrund der Verarbeitung bestehenden Risikos für die Rechte und Freiheiten natürlicher Personen, Art. 24 Abs. 1 S. 1 DSGVO. Diese Maßnahmen müssen erforderlichenfalls überprüft und aktualisiert werden, Art. 24 Abs. 1 S. 2 DSGVO. Konsequenterweise ist ein *Verfahren zur regelmäßigen Überprüfung der Wirksamkeit* von Schutzmaßnahmen zur Gewährleistung der Verarbeitungssicherheit Teil der nach Art. 32 Abs. 1 DSGVO zu ergreifenden technischen und organisatorischen Maßnahmen.

Mittels der automatisierten Auswertung von Messdaten aus dem kontinuierlichen Geschäftsbetrieb des Verantwortlichen

20 Koreng/Lachenmann, DatenschutzR-FormHdB, Form. C. I., Anm. 1-58.

21 Selzer, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit, S. 72.

22 Selzer, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit, S. 72.

kann die Einhaltung datenschutzrechtlicher Anforderungen zu jedem gegebenen Zeitpunkt überprüft werden. Sinkt das Datenschutzniveau, beispielsweise aufgrund neuer regulatorischer Pflichten oder sich ändernder Umstände in der Praxis, unter ein vorab definiertes Mindestmaß, das noch mit der DSGVO vereinbar ist, können zusätzliche technische und organisatorische Maßnahmen umgehend ergriffen werden. Sollte im Gegensatz dazu das Metrikensystem ein Datenschutzniveau indizieren, welches über das erforderliche Maß hinausgeht, könnte der Verantwortliche seine dem Datenschutz zugeteilten Ressourcen und Kapazitäten zurückfahren und an anderer Stelle nutzen, ohne unangemessene Risiken für die Rechte und Freiheiten betroffener Personen in Kauf nehmen zu müssen. Die Erforderlichkeit von Nachjustierungen wäre mithin augenblicklich erkennbar und ihre Umsetzung umgehend möglich. Insofern würde der Einsatz eines Metrikensystems eine häufigere und schnellere Skalierung von Datenschutzmaßnahmen, mithin eine effizientere Umsetzung eines angemessen Datenschutzniveaus ermöglichen, als es mittels händischen Audits möglich ist.

Die Möglichkeit, ressourcensparend Datenschutz zu betreiben, ohne unangemessene Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewirken, würde, im Gegensatz zur Bußgeldandrohung, für Verantwortliche zudem ein genuines und positiv konnotiertes Eigeninteresse an einer intensiven und umfassenden Auseinandersetzung mit Datenschutzvorgaben schaffen und könnte dadurch dazu beitragen, dass Datenschutz nicht als Hürde und Bremse des Geschäftsbetriebs, sondern vielmehr als Chance gesehen wird.

6.2 Beschäftigtenverhältnis als spezieller Einsatzbereich

Über diesen Effizienzgewinn hinaus kann der risikobasierte Ansatz der DSGVO durch die Anwendung von Metrikensystemen auch insbesondere im Kontext des Mitarbeiterdatenschutzes eine Stärkung erfahren, wenn Mitarbeiter die Möglichkeit erhalten, über ein Metrikensystem Kenntnis über den Umsetzungsgrad des von ihrem Arbeitgeber umgesetzten Mitarbeiterdatenschutzes zu erhalten. Dies könnte sich insbesondere in Arbeitsumfeldern potenziell positiv auf die Mitarbeiterzufriedenheit auswirken, in denen Mitarbeiter immer mehr zum gläsernen Menschen werden, wie z.B. in der Zustell- und Logistikbranche, in denen häufig über den gesamten Arbeitstag hinweg die Geolokationsdaten der Zusteller/Fahrer verarbeitet werden, um den Geschäfts- und Privatkunden anzuzeigen, wann ein Fahrer bei ihnen sein wird, um die bestellte Ware zuzustellen.

Die ständige Erhebung von Geolokationsdaten der eigenen Mitarbeiter kann dem Arbeitgeber tiefgreifende und hochsensible Informationen über seine Mitarbeiter aufzeigen, u.a. kann die Information des Standortes vor und nach Pausenzeiten sowie Arbeitsbeginn und -ende Rückschlüsse zur Behandlung chronischer Erkrankungen, oder zum politischen oder religiösen Engagement in Vereinen ermöglichen. Während der Arbeitszeit kann die Erhebung von Standortdaten sowie ggf. weiterer personenbeziehbarer Daten der Mitarbeiter zur Leistungskontrolle genutzt werden. All diese Daten machen den Mitarbeiter anfällig für mögliche Benachteiligungen durch den Arbeitgeber.

Über ein Metrikensystem, das den datenschutzkonformen Umgang mit derartigen Daten anzeigt – z.B. die Messung einer ordnungsgemäß durchgeführten Vergröberung der Geolokationsdatenerhebung, die in der Folge keine Rückschlüsse auf ein aufgesuchtes Krankenhaus o.Ä. ermöglicht – kann Mitarbeitern die Sicherheit gegeben werden, nicht zum gläsernen Mitarbeiter zu werden und keine Benachteiligung o.ä. durch ihren Arbeitgeber befürchten zu müssen, die sich auf eine exzessive Datenverarbeitung stützt. Die Möglichkeit, als Mitarbeiter Einblick in die Metrikenauswertung zu nehmen, kann auch gerade deshalb umgesetzt werden, weil das Metrikensystem eben nicht personenbezogene Daten anzeigt, sondern bloße Kennzahlen zur Auswertung des Datenschutzniveaus nutzt und daher von der gesamten Belegschaft eingesehen werden kann.

7 Fazit und Ausblick

Wenn es darum geht, den Umsetzungsgrad des Datenschutzes innerhalb einer Organisation zu beurteilen und eine zuverlässige Faktenbasis für die Implementierung oder Ablehnung von Datenschutzmaßnahmen zu schaffen, scheinen Metrikensysteme eine für die Zukunft erfolgsversprechende Alternative zu händischen Datenschutzaudits zu sein.

Ihre kontinuierlich laufende Überprüfung könnte eine effizientere Skalierung von Datenschutzmaßnahmen in Abhängigkeit von der wechselnden Risikolage ermöglichen, was eine neuartige und intensivierte Umsetzung des risikobasierten Ansatzes bedeuten würde. Aufgrund dieser gesteigerten Reaktionsfähigkeit könnten Verantwortliche eher Datenpannen abwehren oder minimieren, mithin eine effektivere Gefahrenabwehr betreiben und dadurch die Rechte und Freiheiten betroffener Personen wirksamer schützen. Gleichzeitig wäre aber eine ökonomischere Auswahl und Anpassung von Datenschutzmaßnahmen möglich, sodass sich Metrikensysteme, auch aufgrund ihrer im Vergleich zu händischen Audits günstigen Durchführungskosten, für Verantwortliche ressourcensparend auswirken könnten. Ferner könnten datenschutzrechtliche Nachweispflichten ohne Weiteres erfüllt werden. Die Möglichkeit einer Einsichtnahme in das Metrikensystem im organisationsinternen und vertraulichen Kontext könnte hinsichtlich des Mitarbeiterdatenschutzes zu einer Steigerung der Mitarbeiterzufriedenheit führen.

In Zusammenschau dieser Vorteile erscheint die Weiterentwicklung von Datenschutzmetriken bis hin zur vollständig automatisierten Überprüfbarkeit sämtlicher Datenschutzanforderungen dringend geboten. Auch angesichts der zunehmenden Relevanz des Datenschutzes und der strengen Bußgeldandrohungen könnten Metrikensysteme eine Möglichkeit für Organisationen aller Größen darstellen wettbewerbsfähig, zu bleiben.